METHOD AND APPARATUS TO PROTECT MEDIA EXISTING IN AN INSECURE FORMAT

This application claims the benefit of Provisional Patent Applications Serial #60/188,462 filed 3/10/00, incorporated herein by reference.

Technical Field

This invention relates to the field of embedded data, known as watermarks, and copy control for media.

Background of the Invention

Digital content, including audio, video, images, multimedia, etc., is easy to copy and expensive to create. Thus, it is a great target for illegal distribution, defined as piracy. Currently, this piracy is occurring with audio, using MPEG-1 Layer 3 (MP3) bit-rate compression format and the Internet. The MP3 format is used by new artist who want their music freely distributed, as well as by people transforming CD audio into MP3 and possibly illegally distributing it on the Internet. Professional artists and record labels want to stop the second action while allowing the first, and even distribute new content in MP3.

The problem with robust embedded data based methods of protecting content in this insecure format is that they are computationally intense. The prior-art describes numerous examples of such methods using embedded data (a.k.a. watermarks or steganography) that require frequency transformations. Assuming a different watermark is required for each user, player, storage unit and/or content, distributors will need expensive equipment to protect the data and users will

require expensive devices to render the content.

The problem with efficient embedded data methods used to protect the content in this insecure format is that they are easy to remove, even though they can be made robust to duplication, such as utility patent application #09/404291 entitled "Method and apparatus for robust embedded data" submitted on 9/23/99 by Levy, included herein by reference. Removal of embedded data is not a problem if you require the content to contain the embedded data in order to be rendered, but this concept only works in a secure format. In other words, in an insecure format, if the embedded data that informs the rendering device that the content can or cannot be played is removed, the content can always be played. However, with a secure format, removal of the embedded data that informs the rendering device that the content can or cannot be played leaves the content useless since the device cannot render, such as decrypt, the content without this embedded authorization. For example, in MP3, an insecure format where there is a desire to freely distribute content without protection, the removal of the watermark creates useful pirated content.

Cryptology can also be used to secure the content. However, not only is this technique computationally intense since it requires many operations using a large number of bits, but also one can argue that the format has been changed since existing players cannot play the protected content.

Summary of the Invention

This object of this novel process is to efficiently protect content in an insecure format using two different layers of embedding data (referred to as watermarks for ease of understanding).

One watermark is robust and declares that the content is protected. This watermark is embedded when the content is created in the desired format, such as MP3, CD or DVD. This means that the computational intensity of adding the watermark is not an issue because the watermark is only added to the audio once, and copied with the audio by the distributor. This watermark is labeled the Protect watermark.

The other watermark gives the content its rights, i.e. declares that it is okay to play or record the content. It is efficient, and does not need to be difficult to removal, since removing it produces no advantageous results. The efficiency of this watermark is desirable since it must be embedded each time the audio reproduced, such as downloaded on the Internet, possibly to link the content to the user, player, recorder and/or storage device. Thus, it greatly reduces the cost of copy management for the distributor. In addition, it lowers the cost of the portable players, since they only have to find this efficient watermark. This watermark is labeled the Rights Watermark.

To this end, it is desirable to use different types of watermark for each layer and not two different layers of one watermarking technique. For example, it is not desirable to use one watermarking technique where one layer is embedded at a low-level, thus being fragile, and another layer is embedded at a higher-level, thus being robust.

Importantly, non-protected content may contain neither watermark and can be rendered by any device from any storage. Thus, the rendering devices can be both forward and backwards compatible.

The invented apparatus, which implements the described process, includes an analog or digital logic

processor and a storage unit, such a random access memory.

Brief Description of the Drawings

FIG. 1 is an overview of the process of using two watermarks to protect content in an insecure format with minimal increase in computational complexity, and thus cost.

FIG. 2 displays the pseudocode for the embedding process.

FIG. 3 displays the pseudocode for the retrieving process.

FIG. 4 displays the apparatus.

Detailed Description

This invention begins by explaining the terminology. Content refers to the data, including but not limited to audio, video, images and smells. Storage refers to device that stores the data. The term watermark refers to any system of embedding data that is minimally perceived when the content is played, and is also known as steganography. Data embedded in the header, and not hidden within the content is still considered a watermark. Robust methods are difficult to bypass. A pirate is an individual who attempts to illegally copy or distribute the content.

Fig. 1 displays an overview of the invented process. Content **100** exists in an insecure format, which means that non-compliant devices, i.e. devices ignoring copy protection rules, can render the content even if the content declares itself as non-renderable. An intrinsic benefit of an insecure format is that legacy devices, i.e. device created before the copy protection system was defined, can render the protected content. In other words, the system is backwards and

forwards compatible. An example of an insecure format is MP3. Some artists wish to freely distribute their content in this format. However, there are other interested parties who want to distribute their content in the same format without allowing it to be freely copied and redistributed.

The protect watermark **110** declares that the content is protected. The protect watermark **110** must be extremely difficult to remove, and, accordingly, may be computationally intense. Many existing watermark methods meet this description, and future ones will certainly be designed. The rights watermark **120** gives the user rights to render the content. This watermark may link the content to the user, player, recorder and/or storage device. This link would determine if the user may copy and/or play the content. The rights watermark **120** must be a computationally efficient method that is hard to duplicate. Currently, Levy's application, as referenced above, describes how to design embedded data that is hard to duplicate, i.e. transfer between content to give rights to content that should not include these rights. However, it is expected that more duplication resistant watermarks will be produced in the future.

Both watermarks are embedded and retrieved at different times in the reproduction process, as shown in Figs. 1, 2 and 3. The protect watermark **110** is embedded when the audio is created, and copied with the audio when distributed. In addition, the protect watermark **110** is only retrieved when the rights watermark **120** does not exist in the content. Thus, the computational intensity of adding the watermark is not that important.

The rights watermark **120** is embedded when the content is reproduced, such as being distributed,

placed on permanent storage, or encoded to an alternative form by a personal encoding device. The term reproduced refers to the legal transformation or distribution of the content, whereas copying refers to an individual producing an exact bit-for-bit replication of the content for legal or illegal utilization. Since rights watermark **120** is embedded every time the content is reproduced, its efficiency creates a useful reduction in cost for the supporting hardware. Since the rights watermark **120** is embedded after watermark **110** it must be okay to layer the watermarks, as known to be possible with existing technology.

Optimally, the watermarks are search and retrieved in a specific order, as shown in Figs. 1 and 3. First, the content is searched for rights watermark **120** (box **300**). If rights watermark **120** is retrieved (box **310**) the embedded information is evaluated (box **320**). If the embedded information is correct, the desired action is enabled (box **330**). Alternatively, if the embedded information is not correct, the desired action is disabled (box **340**). Only if rights watermark **120** is not found does the content need to be searched for the computationally intense protect watermark **110** (box **350**). If protect watermark **110** declares the content protected, then the desired action is disabled (box **340**), otherwise the desire action is allowed (box **330**).

When using a rendering device, such as a MP3 player, which has a portable section, the watermark processing tasks can be split between the loader, potentially a PC program, and the portable section. The split can be designed such that the portable section never needs to retrieve the protect watermark, thus reducing the price of the consumer electronics portable player by reducing required processing power

in this portable section. For example, when loading the content to the portable section, the loader can check for the rights watermark and the protect watermark, if necessary. If the desired action for the content is not allowed, the content is not loaded. If the desired action is allowed, the content is loaded to the portable device.

Then, the portable device may only required to process the rights watermark, which is efficient to retrieve and embed, for future actions. The portable section would check for the rights watermark **120** if the rights watermark **120** contained information the portable device is required to understand, such that the portable device can intelligently (i.e. based upon an rules engine) decide how to act upon the content. For example, utility patent application Serial #09/522,312 entitled "Method and apparatus for automatic ID management" submitted on 3/9/00 by Levy (included herein by reference), requires that the portable section (i.e. portable player) requires the user ID contained in the rights watermark such that the portable section can track usage and intelligently limit it to a specified number of users, while allowing all content to be previewed.

Finally, this invented process can be used to restrict copying and/or playing of the content. Since this content is easily created by individuals and desired to exist on storage in general purpose computers, it is preferred to use the invention to restrict playing.

Fig. 4 shows the hardware apparatus required to implement the invented processes, such as embedding and detecting the protect watermark **110** and rights watermark **120**. The hardware includes a logic processor **400** and a storage unit **410**. The logic processor **400** may

be defined as the equivalent of a digital signal processor (DSP), general-purpose central processing unit (CPU), or a specialized CPU, including media processors. A likely DSP chip is one of the Texas Instruments TMS320 product line. A CPU could include one of Intel's Pentium line or Motorola/IBM's PowerPC product line. The design is simple for someone familiar with the state of the art given the above pseudocode and description. The storage unit **410** includes RAM when using a digital processor.

In addition, a person familiar with the state of the art could implement the process with analog and digital circuitry, either separate or in an application specific integrated circuit (ASIC). The analog and digital circuitry could include any combination of the following devices: a digital-to-analog converter (D/A), comparators, sample-and-hold circuits, delay elements, analog-to-digital converter (A/D), and programmable logic controllers (PLC).

The foregoing descriptions of the preferred embodiments of the invention have been presented to teach those skilled in the art how to best utilize the invention. Many modifications and variations are possible in light of the above teaching. For example, even though this invention discusses audio and the Internet, it is extendable to other types of content and distribution. To this end, the following claims define the scope and spirit of the invention.